UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/552,374	07/31/2006	Takashi Satomura	92478-6900	8790

52044 7590 02/17/2009
SNELL & WILMER L.L.P. (Panasonic)
600 ANTON BOULEVARD
SUITE 1400
COSTA MESA, CA 92626

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2431	
MAIL DATE	**DELIVERY MODE**
02/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/552,374	**Applicant(s)** SATOMURA ET AL.
	Examiner LONGBIT CHAI	**Art Unit** 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 October 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/7/2005*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 10/7/2005 but is a 371 case of PCT/JP04/05205 application filed 4/12/2004.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bones et al. (U.S. Patent 7,260,838), in view of Ichihara (U.S. Patent 6,496,937).

As per claim 1 and 33 – 34, Bones teaches management server device that instructs each of a plurality of application devices, which stores a same password therein, to update the password, each application device providing a service to a user who is authenticated using the password (Bones: Column 2 Line 5 – 8, Column 7 line 34 – 36 / Line 56 – 58, Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20: a single sing-on system associated with a cluster of application devices / servers using the same password for all target applications), the management server device comprising:

a first unit operable to have all the application devices attempt to update the password (Bones: Figure 5 / Element 502, Column 2 Line 5 – 8, Column 7 Line 56 – 58 and Column 12 Line 1 – 3: user's desire to update the password across the system).

However, Bones does not disclose expressly a second unit operable to judge whether each application device is capable of updating the password based on a result of the attempt by the application device.

Ichihara teaches a second unit operable to judge whether each application device is capable of updating the password based on a result of the attempt by the application device (Ichihara: Column 3 Line 51 – 55 / Line 10 – 20: the password updating apparatus judges whether the completion of updating of the password is either confirmed or not notified from other computers and if not confirmed, the password can be restored accordingly).

a third unit operable, if at least one of the application devices is not capable of updating the password, to have all the application devices keep the password non-updated (Ichihara: Column 3 Line 51 – 55 / Line 10 – 14: the password is restored if it is failed to be completely updated) & (Bones: Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20: maintaining a same password in a SSO environment having multiple application servers).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ichihara within the system of Bones because (a) Bones teaches incorporating password change policy into a single sing-on system associated with a cluster of application devices / servers using the same password for all target application servers (Bones: Column 2 Line 5 – 8, Column 7 line 34 – 36 / Line 56 – 58), and (b) Ichihara teaches password updating mechanism including requesting, updating and restoring the desired passwords (Ichihara: Column 3 Line 51 – 55 / Line 10 – 20).

As per claim 20, Bones teaches an application device that provides a service to a user who is authenticated using a password, and updates the password based on an instruction from a management server device (Bones: Column 2 Line 5 – 8, Column 7 line 34 – 36 / Line 56 – 58: a single sing-on system associated with a cluster of application devices / servers using the same password for all target applications), the application device comprising:

an authentication password storing unit operable to store an authentication password used for authenticating the user (Bones: Column 1 Line 49 – 51: a password allowing users to access a protected resource is qualified as an authentication password).

However, Bones does not disclose expressly a receiving unit operable to receive a restoration instruction for restoring the password from the management server device.

Ichihara teaches a receiving unit operable to receive a restoration instruction for restoring the password from the management server device (Ichihara: Column 3 Line 51 – 55 / Line 10 – 20: the password updating apparatus <u>judges</u> whether the completion of updating of the password is either confirmed or not notified from other computers and if not confirmed, the password can be restored accordingly).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ichihara within the system of Bones because (a) Bones teaches incorporating password change policy into a single sing-on system associated with a cluster of application devices / servers using the same password for all target application servers (Bones: Column 2 Line 5 – 8, Column 7 line 34 – 36 / Line 56 – 58), and (b) Ichihara teaches password updating mechanism including requesting, updating and restoring the desired passwords (Ichihara: Column 3 Line 51 – 55 / Line 10 – 20).

an old password storing unit operable to store the password that is not updated (Bones: Column 8 Line 39 – 42 & Ichihara: Column 4 Line 10 – 14: old passwords are retrieved from the password history stores);

a writing unit operable to read out the password from the old password storing unit, and overwrite the authentication password with the read-out password (Bones: Column 8 Line 52 – 53: modifying the password is indeed writing the password).

As per claim 26, Bones teaches a password changing system that includes a user device, a plurality of application devices each storing a password and providing a service to a user who is authenticated using the password, and a management server device instructing each of the application devices to update the password (Bones: Column 2 Line 5 – 8, Column 7 line 34 – 36 / Line 56 – 58, Column 1 Line 38 – 40 /

Line 45 – 47 and Column 3 Line 14 – 20: a single sing-on system associated with a cluster of application devices / servers using the same password for all target applications), wherein the management server device comprises:

a first unit operable to have all the application devices attempt to update the password (Bones: Figure 5 / Element 502, Column 2 Line 5 – 8, Column 7 Line 56 – 58 and Column 12 Line 1 – 3: user's desire to update the password across the system).

However, Bones does not disclose expressly a second unit operable to judge whether each application device is capable of updating the password based on a result of the attempt by the application device.

Ichihara teaches a second unit operable to judge whether each application device is capable of updating the password based on a result of the attempt by the application device (Ichihara: Column 3 Line 51 – 55 / Line 10 – 20: the password updating apparatus judges whether the completion of updating of the password is either confirmed or not notified from other computers and if not confirmed, the password can be restored accordingly).

a third unit operable, if at least one of the application devices is not capable of updating the password, to have all the application devices to keep the password non-updated (Ichihara: Column 3 Line 51 – 55 / Line 10 – 14: the password is restored if it is failed to be completely updated) & (Bones: Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20: maintaining a same password in a SSO environment having multiple application servers).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ichihara within the system of Bones because (a) Bones teaches incorporating password change policy into a single sing-on system associated with a cluster of application devices / servers using the same password for all target application servers (Bones: Column 2 Line 5 – 8, Column 7 line 34 – 36 / Line 56 – 58), and (b) Ichihara teaches password updating mechanism including requesting, updating and restoring the desired passwords (Ichihara: Column 3 Line 51 – 55 / Line 10 – 20).

each application device comprises:

an old password storing unit operable to store the password that is not updated (Bones: Column 8 Line 39 – 42 & Ichihara: Column 4 Line 10 – 14: old passwords are retrieved from the password history stores);

an authentication password storing unit operable to store an authentication password used for authenticating the user (Bones: Column 1 Line 49 – 51: a password allowing users to access a protected resource is qualified as an authentication password);

a receiving unit operable to receive a restoration instruction for restoring the password, which is not updated, from the management server device (Ichihara: Column 3 Line 51 – 55 / Line 10 – 14: the password is restored if it is failed to be completely updated); and

a writing unit operable to read out the password, which is not updated, from the old password storing unit, and overwrite the authentication password with the read-out password (Bones: Column 8 Line 52 – 53: modifying the password is indeed writing the password).

As per claim 2, Bones as modified teaches a fourth unit operable to receive a password update request from a user device, wherein the first unit has all the application devices attempt to update the password based on the password update request (Bones: Column 7 line 34 – 36 / Line 56 – 58, Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20).

As per claim 3, Bones as modified teaches the first unit instructs all the application devices to update the password, the second unit judges whether the password has been successfully updated by each application device, and the third unit instructs, if any of the application devices has failed to update the password, the other application devices, which have successfully updated the password, to restore the password (Bones: Column 2 Line 5 – 8, Column 7 line 34 – 36 / Line 56 – 58, Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20).

As per claim 4 and 8, Bones as modified teaches the fourth unit receives the password update request that includes the password and a new password (Bones: Column 7 Line 56 – 58), and the first unit generates a password update instruction that includes the password and the new password, and transmits the password update instruction to each application device (Bones: Column 2 Line 5 – 8).

As per claim 5, Bones as modified teaches a response receiving subunit operable to receive a response that indicates an update success or an update failure from each application device; and a determining subunit operable to determine, if the response indicates the update success, that the application device, from which the judging subunit receives the response, has successfully updated the password, and to determine, if the response indicates the update failure, that the application device has failed to update the password (Ichihara: Column 3 Line 51 – 55 / Line 10 – 20: the password updating apparatus judges whether the completion of updating of the password is either confirmed or not notified from other computers and if not confirmed, the password can be restored accordingly).

As per claim 6 and 10, Bones as modified teaches a timer subunit operable to count elapsed time; an initializing subunit operable to reset the counted elapsed time to an initial value when the first unit transmits the password update preparing instruction; a waiting subunit operable to wait for the response to be transmitted from each application device, and receive the response if the response is transmitted; a judging subunit operable to judge whether the counted elapsed time is more than a predetermined threshold value; and a determining subunit operable, in the case where the counted elapsed time is equal to or smaller than the threshold value and the waiting subunit has received the response that indicates the update preparation completion, to determine that the application device, from which the waiting subunit has received the response, has already prepared to updated the password, and operable, in the other cases, to determine that the application device has not prepared yet to update the password (Ichihara: Column 4 Line 32 – 33 / Line 41 – 43: a timer must be needed to detect a confirmation response is missing).

As per claim 7, Bones as modified teaches the first unit instructs all the application devices to prepare to update the password, the second unit judges whether each application device has already prepared to update the password, and the third unit cancels, if at least one of the application devices has not prepared to update the password yet, the instruction to prepare to update the password for the other application devices which have already prepared to update the password (Ichihara: Column 3 Line 51 – 55 / Line 10 – 14: the password is restored if it is failed to be completely updated) & (Bones: Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20: maintaining a same password in a SSO environment having multiple application servers).

As per claim 9, Bones as modified teaches a response receiving subunit operable to receive a response that indicates an update preparation completion or an update preparation incompletion from each application device; and a determining subunit operable to determine, if the response indicates the update preparation completion, that the application device, from which the judging subunit receives the response, has already prepared to update the password, and to determine, if the response indicates the update preparation incompletion, that the application device has not prepared yet to update the password (Ichihara: Column 3 Line 51 – 55 / Line 10 – 14: the password is restored if it is failed to be completely updated) & (Bones: Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20: maintaining a same password in a SSO environment having multiple application servers).

As per claim 11, Bones as modified teaches a message transmitting unit operable to transmit a message, indicating that the password should be restored, to the user device, if the second unit judges in the negative concerning any of the application devices (Ichihara: Column 3 Line 51 – 55 / Line 10 – 14: the password is restored if it is failed to be completely updated) & (Bones: Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20: maintaining a same password in a SSO environment having multiple application servers).

As per claim 12, Bones as modified teaches a management storing unit operable to store information as to whether each application device is currently being maintained, wherein the first unit has all the application devices update the password if no application device is currently being maintained (Bones: Figure 8 / Element 806, 814, 820 and 826, Column 6 Line 32 – 36, Column 10 Line 3 – 26 and Column 10 Line 59 – 67: if password policy is not found then use default change password policy to change passwords).

As per claim 13, Bones as modified teaches the first unit stops updating the password if any of the application devices is currently being maintained, and the management server device further comprises a message transmitting unit operable to transmit a message, indicating that the update of the password should be stopped, to the user device (Ichihara: Column 3 Line 35 – 37: a current password storage is used to eliminate the need of updating the password).

As per claim 14 and 15, Bones as modified teaches the application devices are connected to the management server device via a first network, and the user device is connected to the management server device via a second network that is not connected to the first network (Bones: Column 3 Line 10 – 25).

As per claim 14, 15, 18, 23, 25, 28, 29 and 32, Bones as modified teaches the application devices are connected to the management server device via a first network, and the user device is connected to the management server device via a second network that is not connected to the first network (Bones: Column 3 Line 10 – 25).

As per claim 16, 24 and 30, Bones as modified teaches the management server device is connected to the application devices via dedicated lines respectively, the management server device transmits and receives information, which is used for updating the password, to and from the application devices via the dedicated lines, and information used for providing the services is received and transmitted via the first network and the second network (Bones: Column 3 Line 10 – 25 and Examiner notes Official Notice is taken that the use of a dedicated line is a well-known secure communication path on said communication medium).

As per claim 17 and 31, Bones as modified teaches the application devices and the user device are connected to the management server device via a network, and the management server device further comprises: a storing unit operable to store an association table in which types of the applications and positions of the application devices on the network are associated to each other on a one-to-one basis; a receiving unit operable to receive type information indicating an application type and procedure information indicating details of a procedure; an obtaining unit operable, using the association table, to obtain a position of an application device corresponding to the received type information; and a transmitting unit operable to transmit the procedure information to the application device whose position is obtained by the obtaining unit (Bones: Figure 9 Element 908 and Column 10 Line 63 – 67: (a) a password list is qualified as a table of passwords associated with target application devices (b) a password policy is qualified as a procedure).

As per claim 19, Bones as modified teaches a new password updated from the password is an initial password assigned to the user, the first unit has all the application devices attempt to update the password to the initial password (Bones: Column 1 Line 62 – 64); the second unit judges whether each application device is capable of updating the password to the initial password (Bones: Column 1 Line 62 – 64 and Column 12 Line 7); and if at least one of the application devices is not capable of updating the password to the initial password, the third unit has all the application devices keep the password non-updated (Ichihara: Column 3 Line 51 – 55 / Line 10 – 14: the password is restored if it is failed to be completely updated) & (Bones: Column 1 Line 38 – 40 / Line 45 – 47 and Column 3 Line 14 – 20: maintaining a same password in a SSO environment having multiple application servers).

As per claim 21 and 27, Bones as modified teaches the application device receives and transmits information relating to the service from and to a user device via the management server device (Bones: Column 3 Line 14 – 25, Column 2 Line 5 – 8, Column 7 Line 56 – 58 and Column 12 Line 1 – 3).

As per claim 22, Bones as modified teaches if currently being maintained, the application device notifies the management server device that the application device is currently being maintained (Ichihara: Column 3 Line 32 – 33: a password is currently being maintained to eliminate the need of updating the password) & (Bones: Figure 9 Element 908 and Column 10 Line 63 – 67).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Patent Examiner
Art Unit 2431
7/8/2008